HOME COMPUTER SECURITY 103 BUILDING SAFE AND SECURE NETWORKS AT HOME

A Workshop by the City of Seattle

Office of Information Security

Roadmap for this Presentation

- Introductions
- Brief Review of 101 & 102
- Intro to IP Networks
  - Types
  - Hardware
  - Communications
- Secure Network Configuration
  - Wired
  - Wireless

Introductions

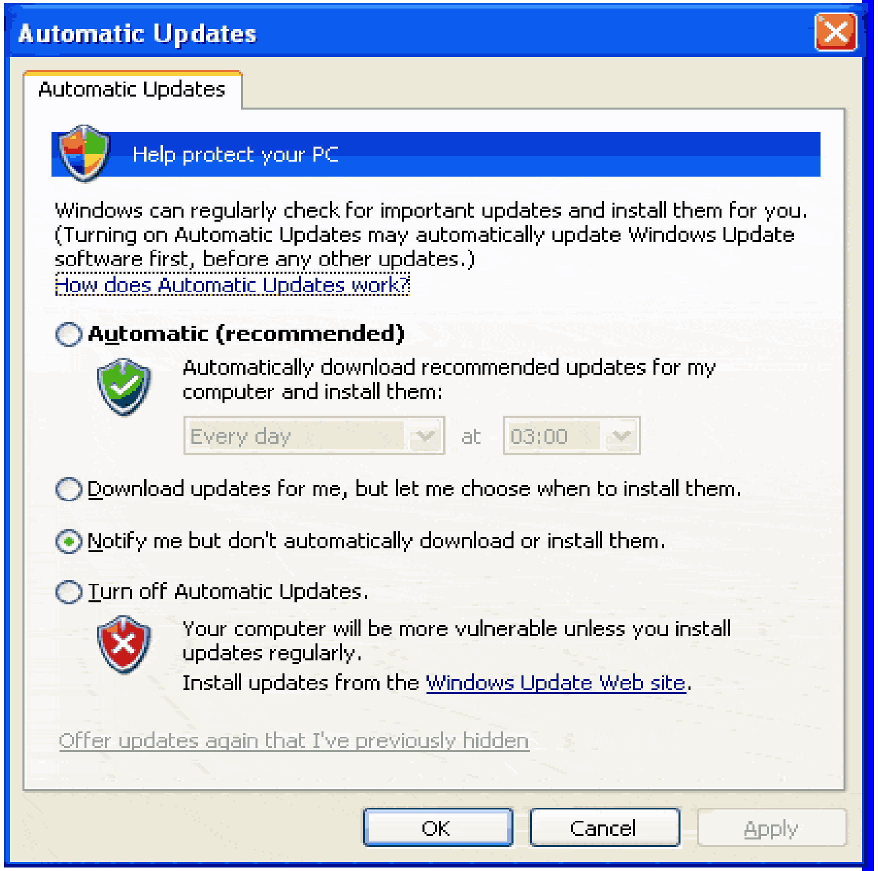
- The Office of Information Security (OIS)
  - Who we are
  - What we do

Review (101)

- Information Security 101
  - Threats from E-mail and Internet use
    - Phishing, Pump-n-dump, 419
    - Botnets, Malware
    - Social Engineering
    - Drive by web attacks
    - Web 2.0 (social networking) issues
  - Tips to stay safe
    - Be aware
    - Be alert
    - Be prepared and informed

Review (102)

- Tools and Tips
  - Anti-virus, Anti-Malware
  - Patching & Updates
  - Firewalls
  - Browser Configuration
  - Encryption
  - Backups



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

○ **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 03:00

○ Download updates for me, but let me choose when to install them.

● Notify me but don't automatically download or install them.

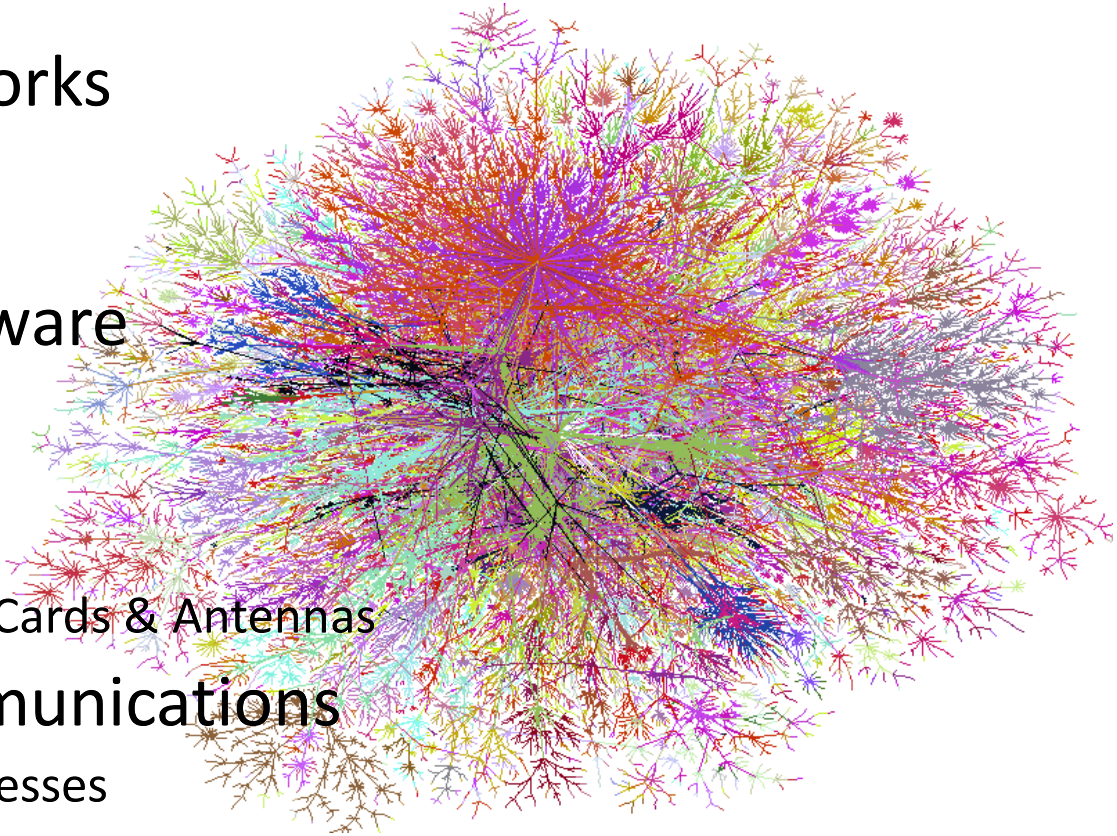
○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

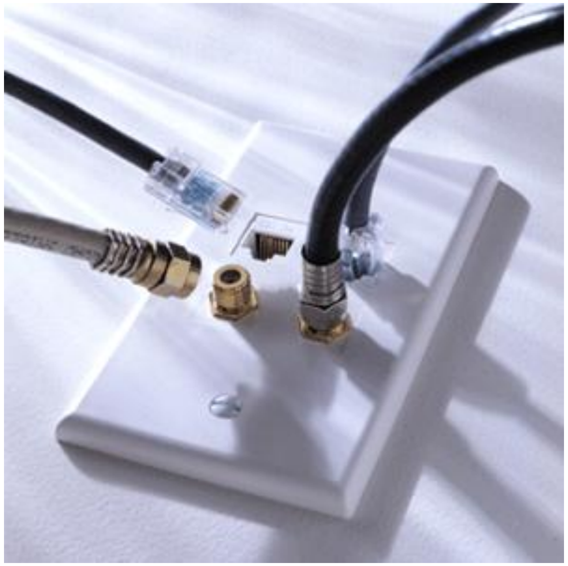
Offer updates again that I've previously hidden

Introduction to IP Networks



- Types of Networks
  - Wired
  - Wireless
- Network Hardware
  - Modems
  - Routers
  - Cabling
  - Wireless Access Cards & Antennas
- Network Communications
  - IP and Mac Addresses
  - NAT
  - Packets
  - OSI Layers
  - TCP vs UDP

Wired vs Wireless Networks



- Wired
  - Modem to router to computer
  - Connected via cable
- Wireless
  - Modem to router/access point
  - Then antenna to antenna (access cards)
  - Varieties of signal quality and range
    - 802.11a, b, **g**, n
  - Security Issues

Network Hardware (1)

- Modems (modulator – demodulator)
  - Connection to Internet
  - Cable, DSL, Dial-up
  - Can convert analog to digital
- Router
  - Routes data to addresses internal and external
  - Can act as firewall
  - Often does DNS (domain name service)

Network Hardware (2)

- Cabling
  - Category 5 (often called Cat 5)
  - Unshielded twisted pair (UTP)
  - RJ45 connectors

- Wireless Access Cards/Antennas
  - Often internal on newer laptops
  - Can be external
  - Can build your own for longer range or snooping!

- VOIP Routers
  - Allow telephone connections over an IP network

Network Communications (1)

- OSI Model (Open Systems Interconnection)
  - Application, Presentation, Session, Transport, Network, Data Link, and Physical
  - Network communications happen from Transport on down
    - Physical = cable, routers, access points, etc.
    - Link = data transfer protocols between network hardware
    - Network = routing protocols and functions
    - Transport = transfer of data – reliability and error control (TCP and UDP)

Network Communications (2)

- Ethernet
  - Defines standards for networks
  - Specifically for physical and data link layers
    - How to complete data transfer
    - Dealing with collisions
    - Use of Cat 5 cabling and specific network hardware
    - 10BASE-T, 100BASETX, and 1000BASE-T (Gigabit)
- Packets
  - Method of delivering data
  - Contains control information and payload
    - Control information includes source and destination, error detection codes and sequencing information
    - User data is actual information you are sending

Network Communications (3)

- Internet Protocol (IP aka TCP/IP)
  - IPv4 (32 bit – 4 billion) vs IPv6 (128 bit – 340 undecillion [3.4 x 10 to the 38th power!])
  - V4 addresses in ‘dot-decimal’ notation – four numbers ranging from 0 – 255, e.g. 156.74.201.16
  - Private network reserved addresses 10.0.0.0, 172.16-32.x.x, 192.168.x.x
- NAT (Network Address Translators)
  - Takes internal private network addresses and modifies them to Internet address or vice versa.
    - Hides internal address space from Internet
    - Rewrites IP packets on exit so they appear to come from one router

Network Communications (4)

- MAC (Media Access Control) Addresses
  - Unique (well sort of) address assigned to network adaptors (network interface cards – NICS)
  - Usually encodes manufacture id numbers
  - Helps to identify different devices on a network
  - Can be (easily) spoofed
- Services and Ports
  - Services are different system level applications (in this case for communications between systems)
    - telnet
    - ftp
    - ssh
  - Ports are communications end-points used by services

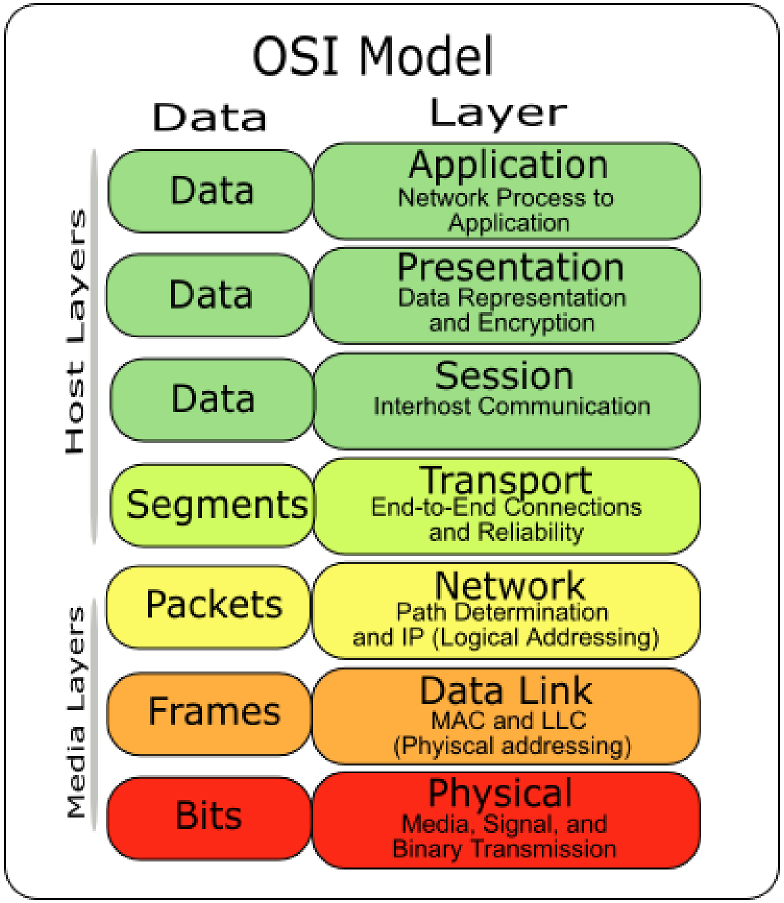
So What's TCP/IP? (and why isn't it SNA/IPX?)

Transport Layer

- Transmission Control Protocol
  - Handles packet fragmentation, reconstruction, retransmission
  - Maintains connection "state"

Network Layer

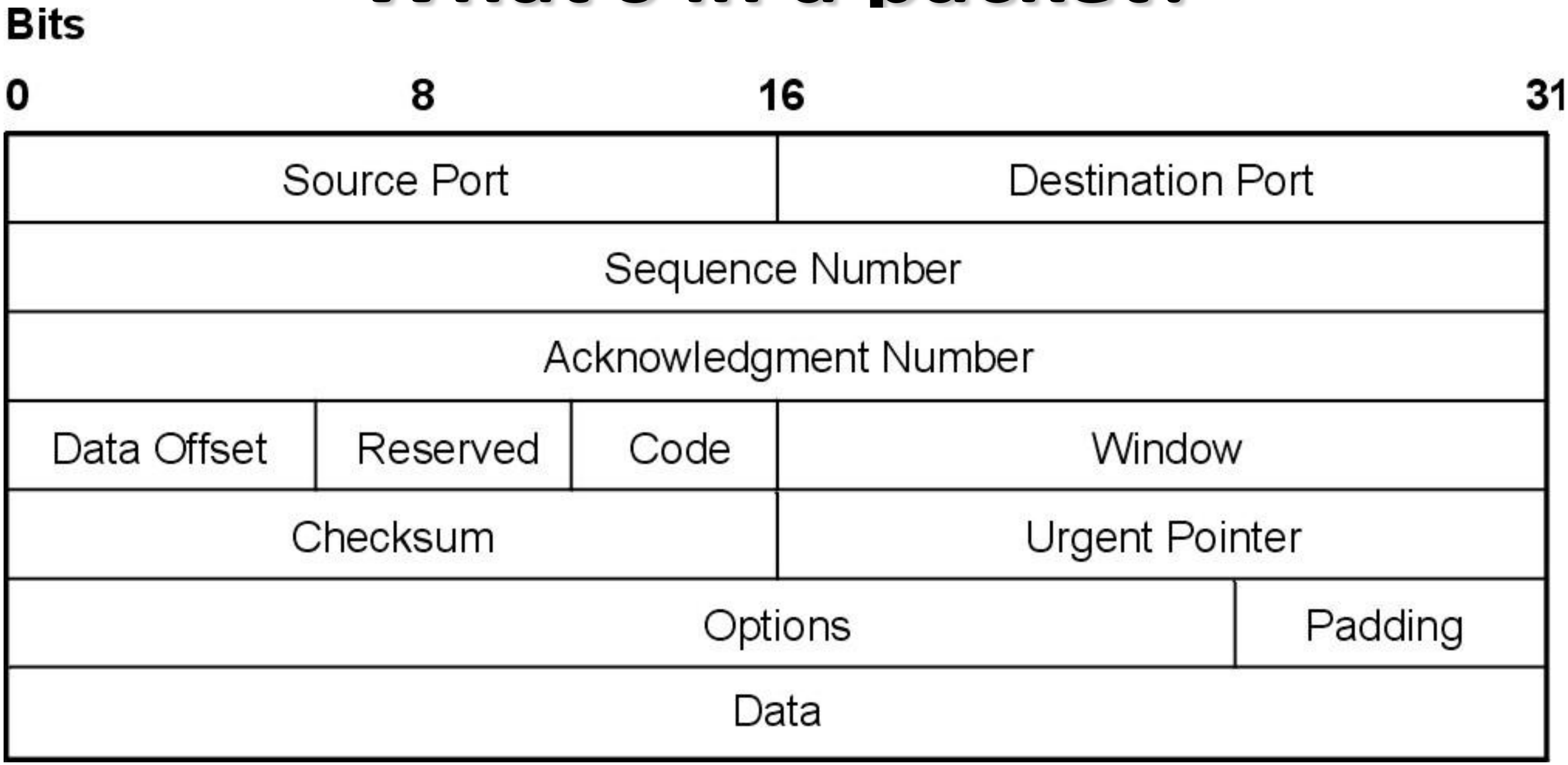
- Internet Protocol
  - Handles the routing of packets from source to destination
  - Relies on unique addresses for each node on the Internet
  - There aren't enough addresses!



OSI Model

	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation and Encryption
	Data	Session Interhost Communication
	Segments	Transport End-to-End Connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical Addressing)
	Frames	Data Link MAC and LLC (Phyiscal addressing)
	Bits	Physical Media, Signal, and Binary Transmission

What’s in a packet?



Bits

0 8 16 31

Source Port | Destination Port

Sequence Number

Acknowledgment Number

Data Offset | Reserved | Code | Window

Checksum | Urgent Pointer

Options | Padding

Data

Everything but “Data” is the packet header

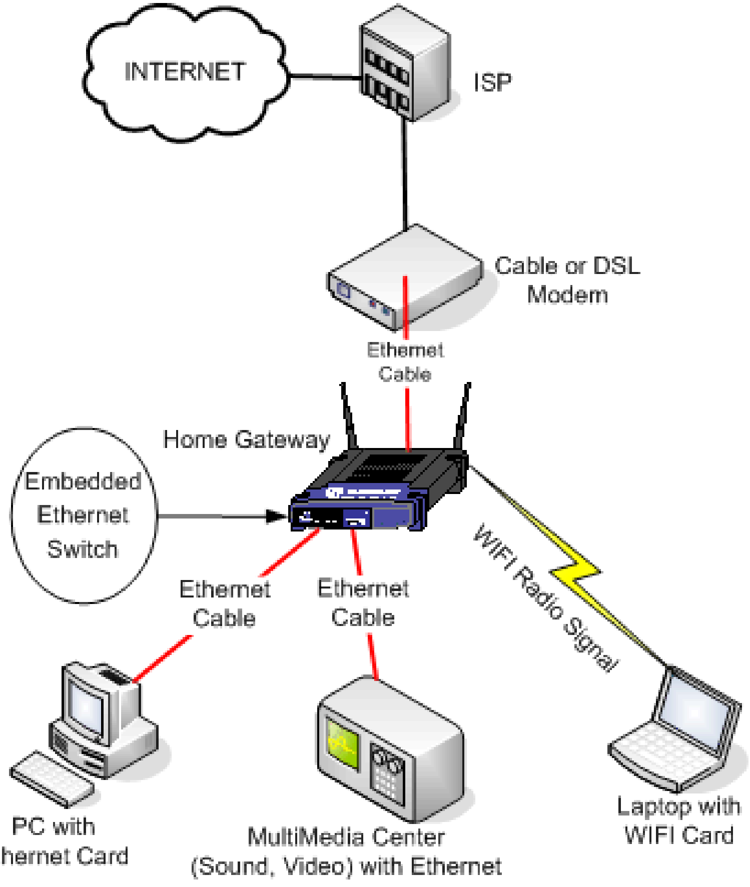
Infrastructure Services

- Dynamic Host Configuration Protocol (DHCP)
  - Gives IP address, netmask, DNS server, default route, etc.
  - Can be configured to limit size of address pool
  - Can be configured to limit based on MAC address
- Routing
  - How do I get a packet from here to my destination?
  - Static vs dynamic routes
- Domain Name System (DNS)
  - Maps a name to an IP address (“A” record)
  - Maps an IP address to a name (“PTR” record)
  - Specifies where to deliver e-mail (“MX” record)
  - If you don’t have a name server specified, there is no Internet

Let’s take a well-deserved break

Secure Setup and Configuration

- Routers and Firewalls
  - Default settings
  - DNS and DHCP
  - Services
  - Remote Access
- Wireless
  - SSID
  - DHCP controls
  - MAC address filtering
  - Encryption
- General best practices
  - Upgrades and patches
  - Backups and documentation
  - Logging and monitoring



Steps

- Choose your internal network addressing
- Install the firewall
  - Change default administrator username and password
  - Configure addressing
  - Configure infrastructure services
  - Configure logging
  - Configure services (optional)
  - Configure remote access (optional)
- Install wireless access point
  - Change default administrator username and password
  - Configure SSID, broadcast, channel, radio
  - Configure WPA2 encryption
  - If no firewall configure DHCP

But First… Why Bother!

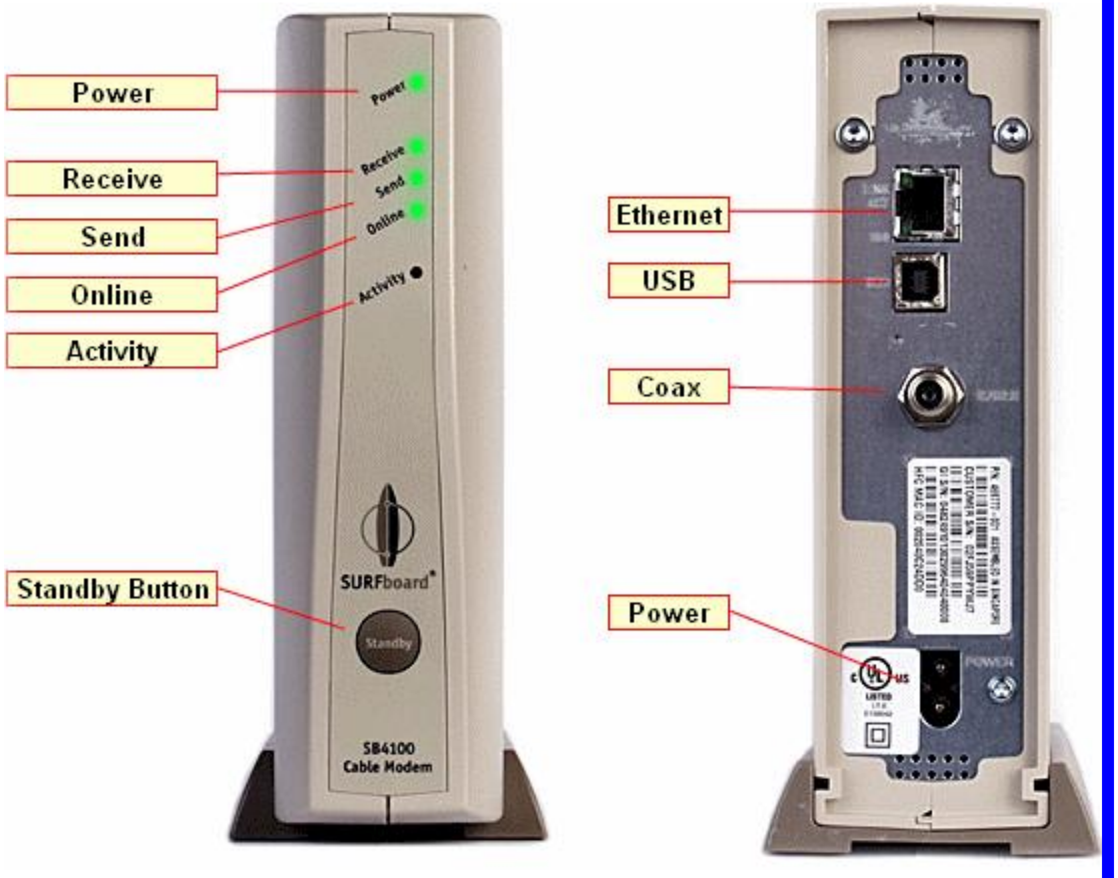
- Attack Traffic
  - Constant, ubiquitous scanning
  - Un-secured devices compromised in 6 minutes or less!
- Man in the Middle
  - Take over your router and all connections to it
  - Router attacks are becoming very prevalent
- If it looks like it's you…
  - Use your Internet access for downloads
  - Cyber stalking or threats
  - Spamming or Denial of Service
- Or maybe they'll BE you…
  - Access to your network is easy
  - So is damage if they feel like it

Cable Modems

- Uses ‘tftp’ service to download configuration and firmware from ISP
- Access the read-only admin interface using a web browser

Can’t change settings on ISP-issued modem, BUT:

- Use for diagnostics
- Buy your own
- “Uncapping”



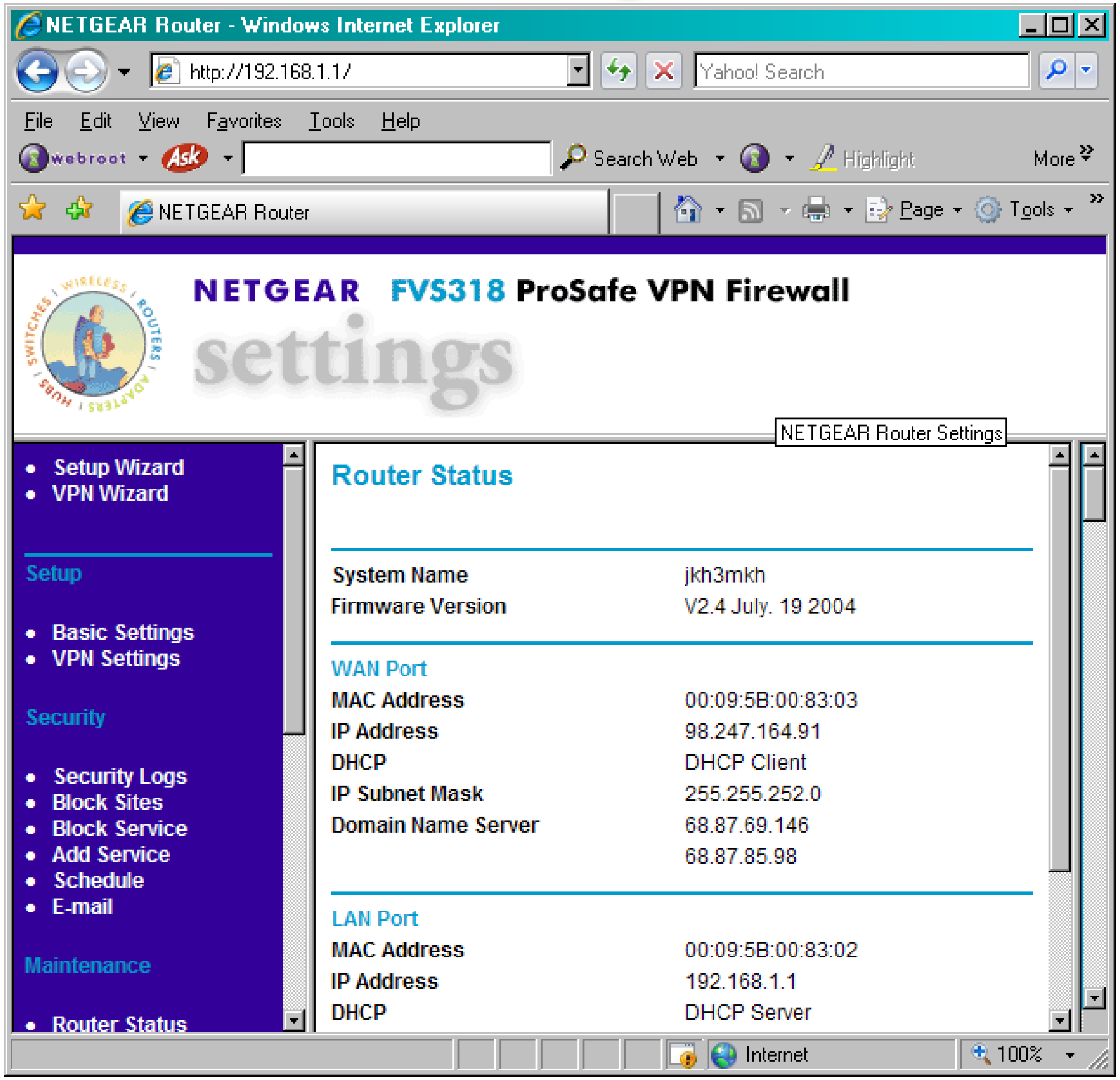
Router/Firewall

- First point of control between you and the Internet
- One internal and one external interface, each in different networks
- The router will, strangely enough, ROUTE packets between the connected networks (if allowed)
- It will also PREVENT packets from being routed

Configuration – Basics

- First, access your router or firewall – usually from browser go to: 192.168.1.1
- **Immediately change the default administrator name and password!**
- THEN plug connect the router/firewall and cable modem
- Record the IP address the firewall has been assigned for the WAN interface, the IP address of the cable modem, and DNS servers
- Change your internal network interface address if desired – make it 10.1.1.1 or 10.9.8.7 or 172.19.0.1
- Set it up as a DHCP server; make the size of your DHCP address pool equal to the number of devices you intend to have on the network
- Get a MAC address from each device, and filter DHCP requests by MAC address (see example coming with wireless)
- Configure filters (default is to block all inbound; allow all outbound)
- Save (export) the configuration; record all details
- **Did I mention… change the default administrator name and password!**

WAN Configuration



Router Status

System Name	jkh3mkh
Firmware Version	V2.4 July. 19 2004

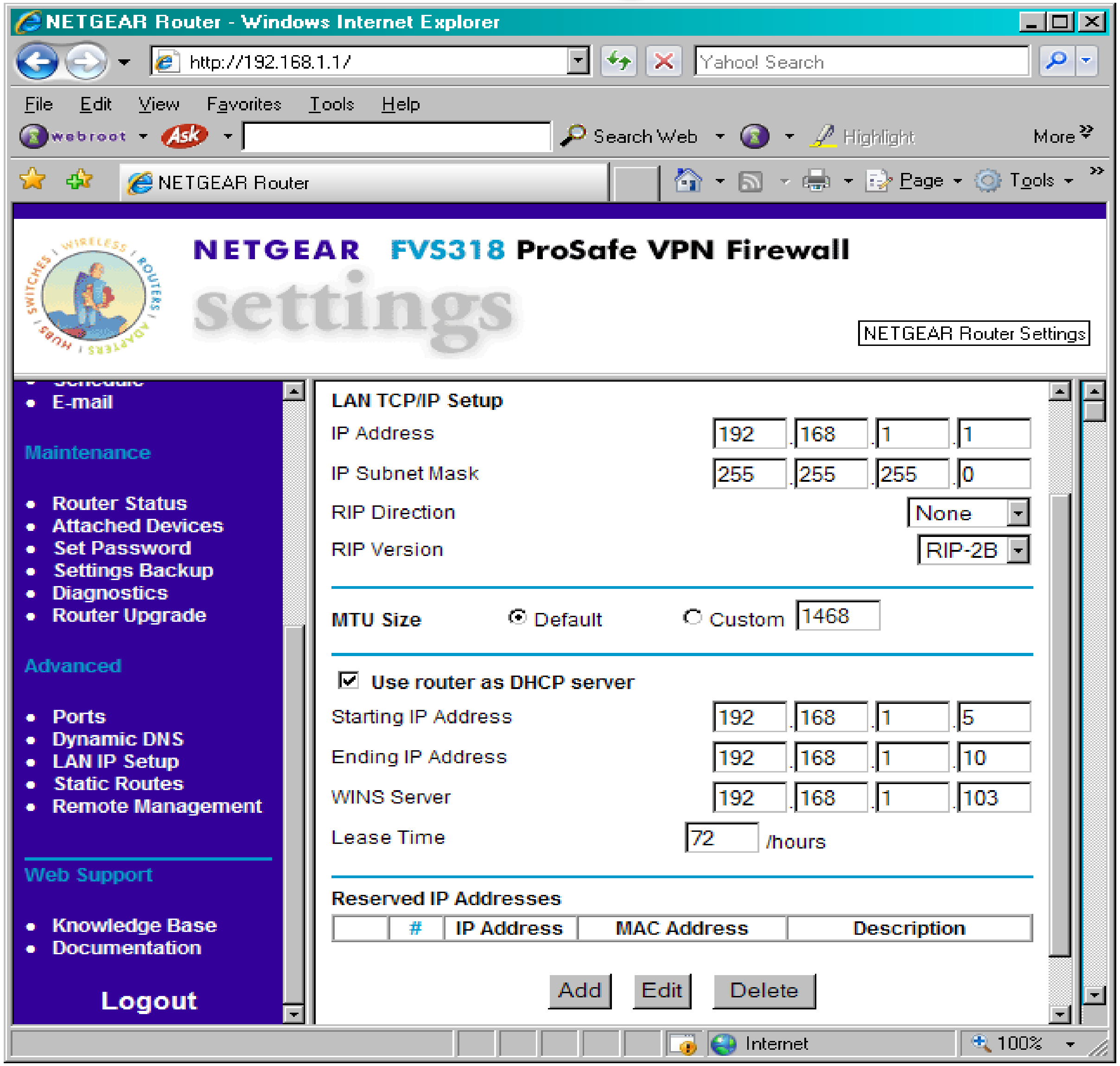
WAN Port

MAC Address	00:09:5B:00:83:03
IP Address	98.247.164.91
DHCP	DHCP Client
IP Subnet Mask	255.255.252.0
Domain Name Server	68.87.69.146 68.87.85.98

LAN Port

MAC Address	00:09:5B:00:83:02
IP Address	192.168.1.1
DHCP	DHCP Server

DHCP Configuration



LAN TCP/IP Setup

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	None
RIP Version	RIP-2B

MTU Size ● Default ○ Custom 1468

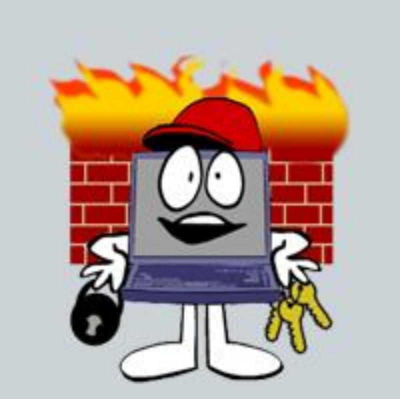
☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 1 . 5
Ending IP Address	192 . 168 . 1 . 10
WINS Server	192 . 168 . 1 . 103
Lease Time	72 /hours

Reserved IP Addresses

	#	IP Address	MAC Address	Description

Configuration – Activity Monitoring

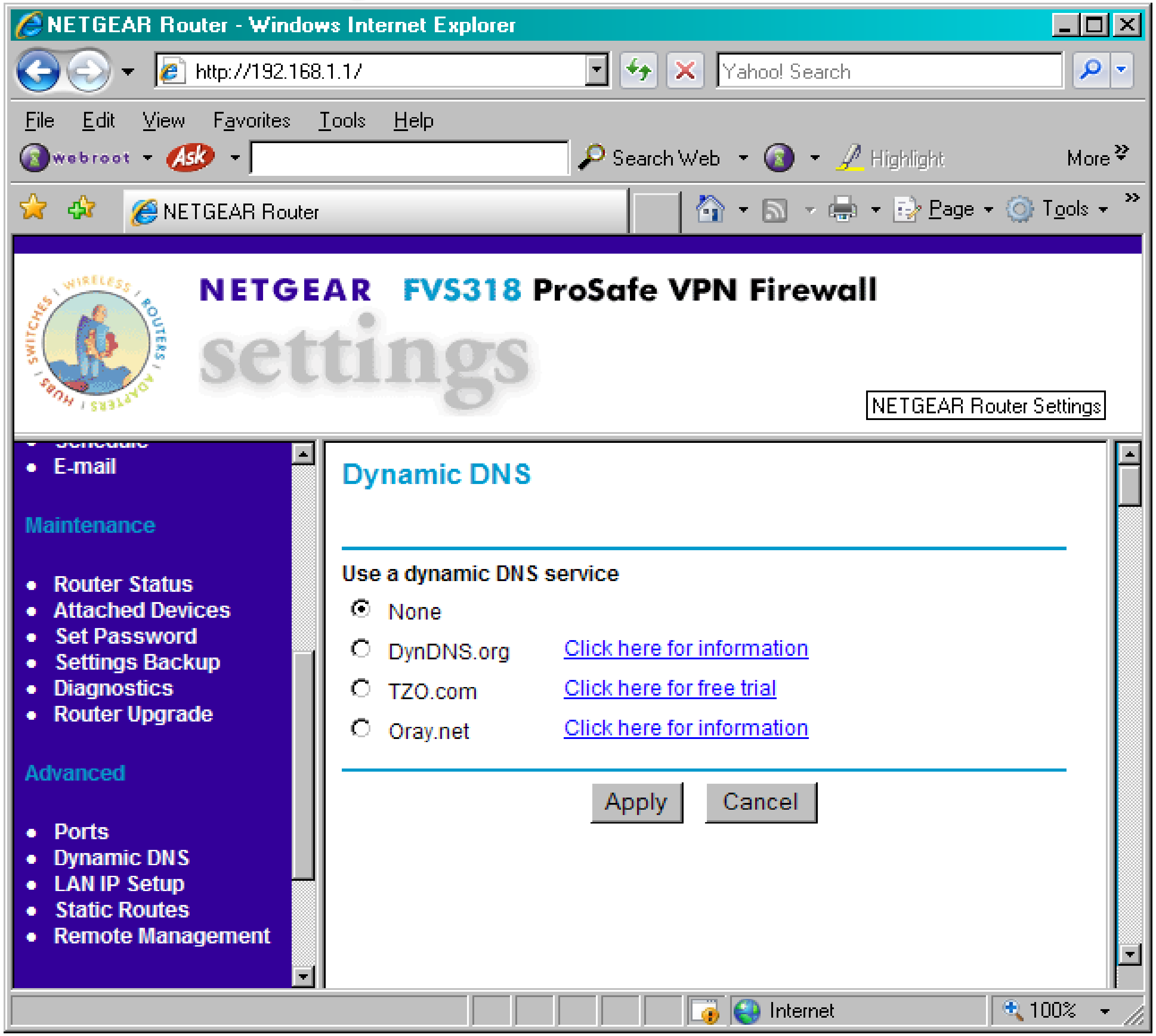


- Logging
  - Make sure logging is enabled
  - Send logs to yourself via email
  - Rotate logs at a frequency that doesn't allow them to overwrite
    - Size limits set so you don't lose data
- Monitoring
  - Schedule regular time to review logs for anomalies
  - Use monitoring tools to help parse and decipher
  - Setup alarms

Optional Configuration

- Subscribe to a dynamic DNS service
- Make internal services available to the Internet
  - Web server (plug through port 80)
  - Mail server (plug through port 25; need MX record in DNS)
  - Remote encrypted access to internal server (plug through port 22)
- Create a “demilitarized zone”, or DMZ network
  - Router/firewall will plug all connection requests for services through to designated internal system
  - Good technique for combination web/mail server
  - Good technique for creating a honeypot
- Remote administration
  - IF and ONLY IF you have a VERY STRONG PASSWORD
  - Even then it’s not a good idea
  - You shouldn’t do this

Dynamic DNS



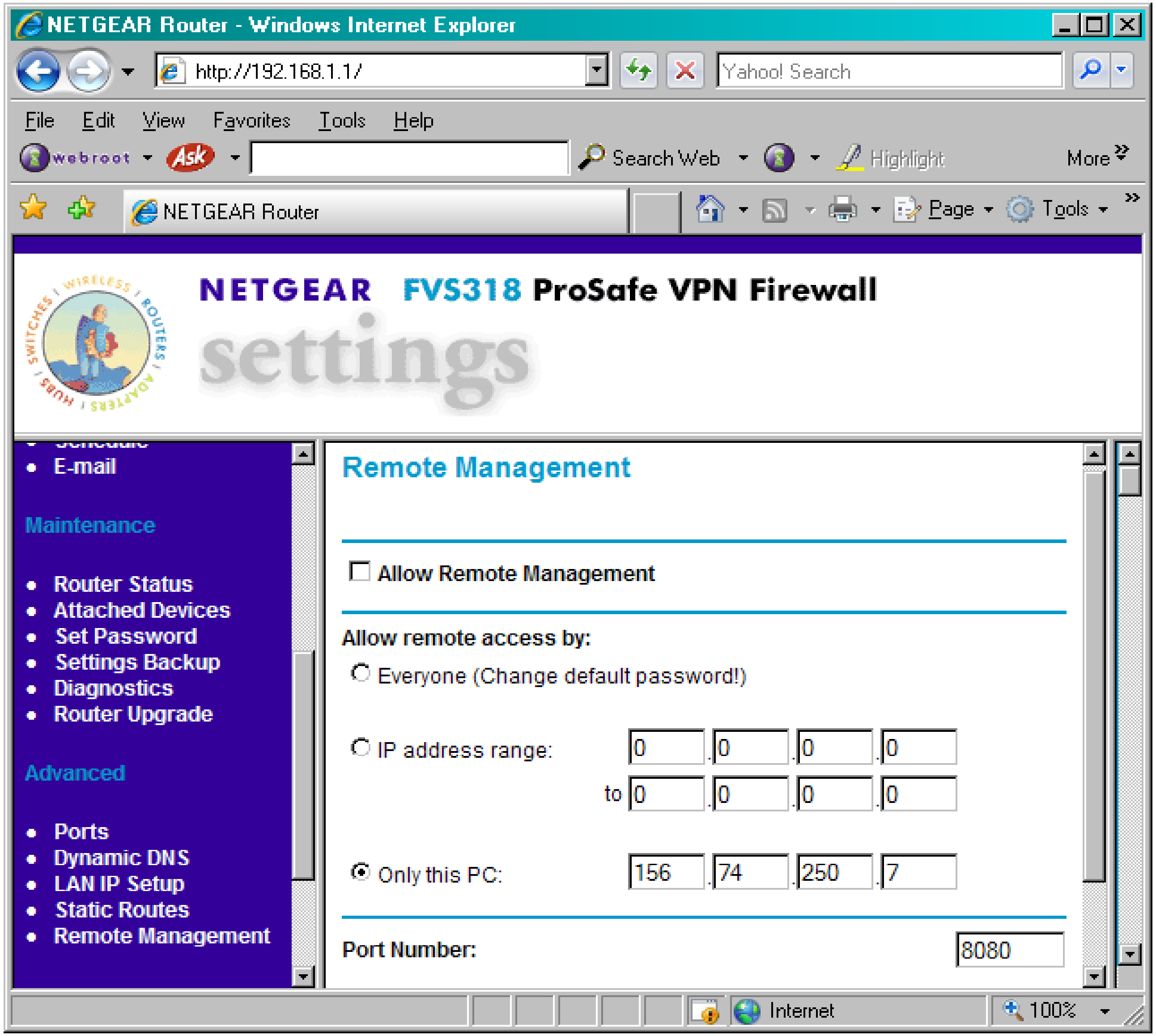
Dynamic DNS

Use a dynamic DNS service

- ● None
- ○ DynDNS.org — Click here for information
- ○ TZO.com — Click here for free trial
- ○ Oray.net — Click here for information

Apply   Cancel

Remote Administration



Remote Management

□ Allow Remote Management

Allow remote access by:

○ Everyone (Change default password!)

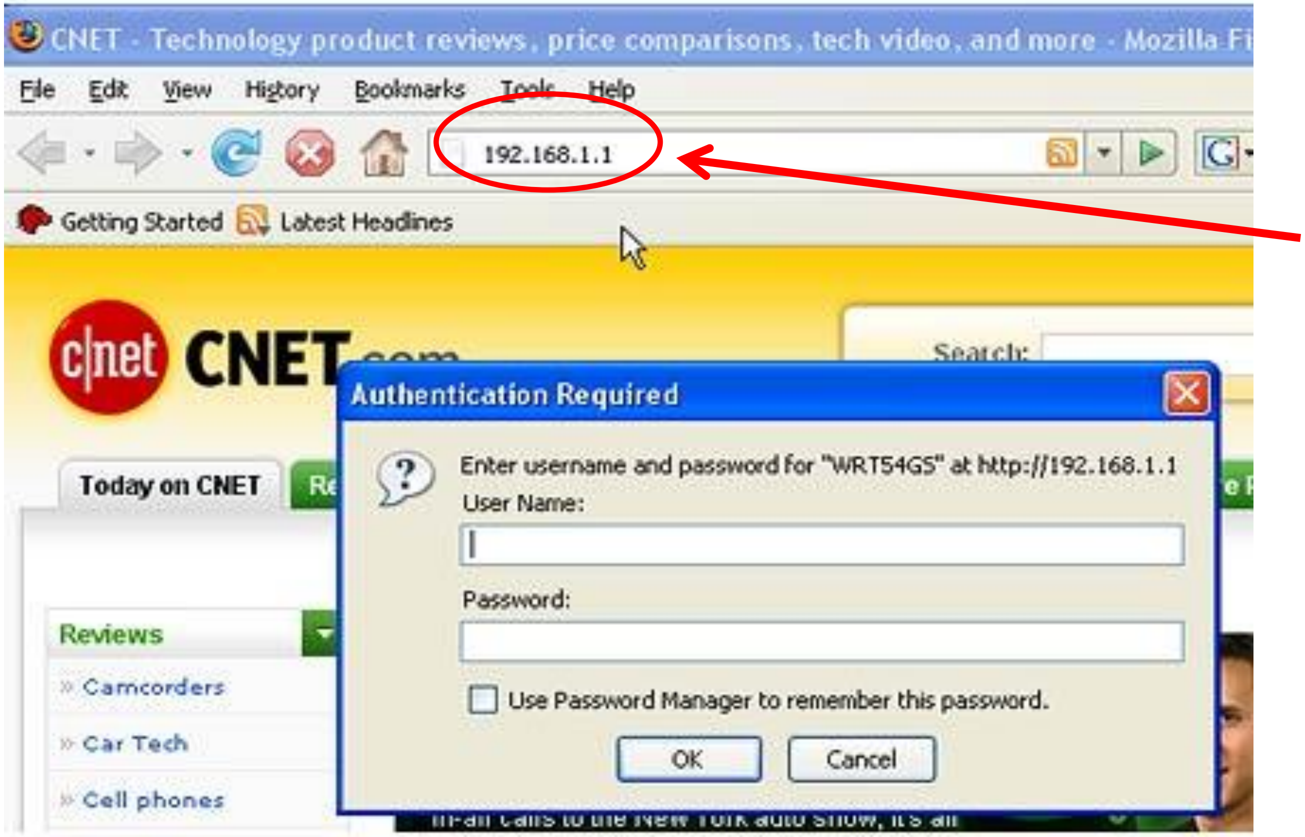
○ IP address range: 0 . 0 . 0 . 0
to 0 . 0 . 0 . 0

● Only this PC: 156 . 74 . 250 . 7

Port Number: 8080

Wireless Security Illustrated (1)

With acknowledgements to CNET Reviews


CNET - Technology product reviews, price comparisons, tech video, and more - Mozilla Fi
File Edit View History Bookmarks Tools Help
192.168.1.1
Getting Started
Latest Headlines
cnet CNET.com
Search:
Today on CNET
Reviews
Camcorders
Car Tech
Cell phones

Authentication Required

Enter username and password for "WRT54GS" at http://192.168.1.1

User Name:

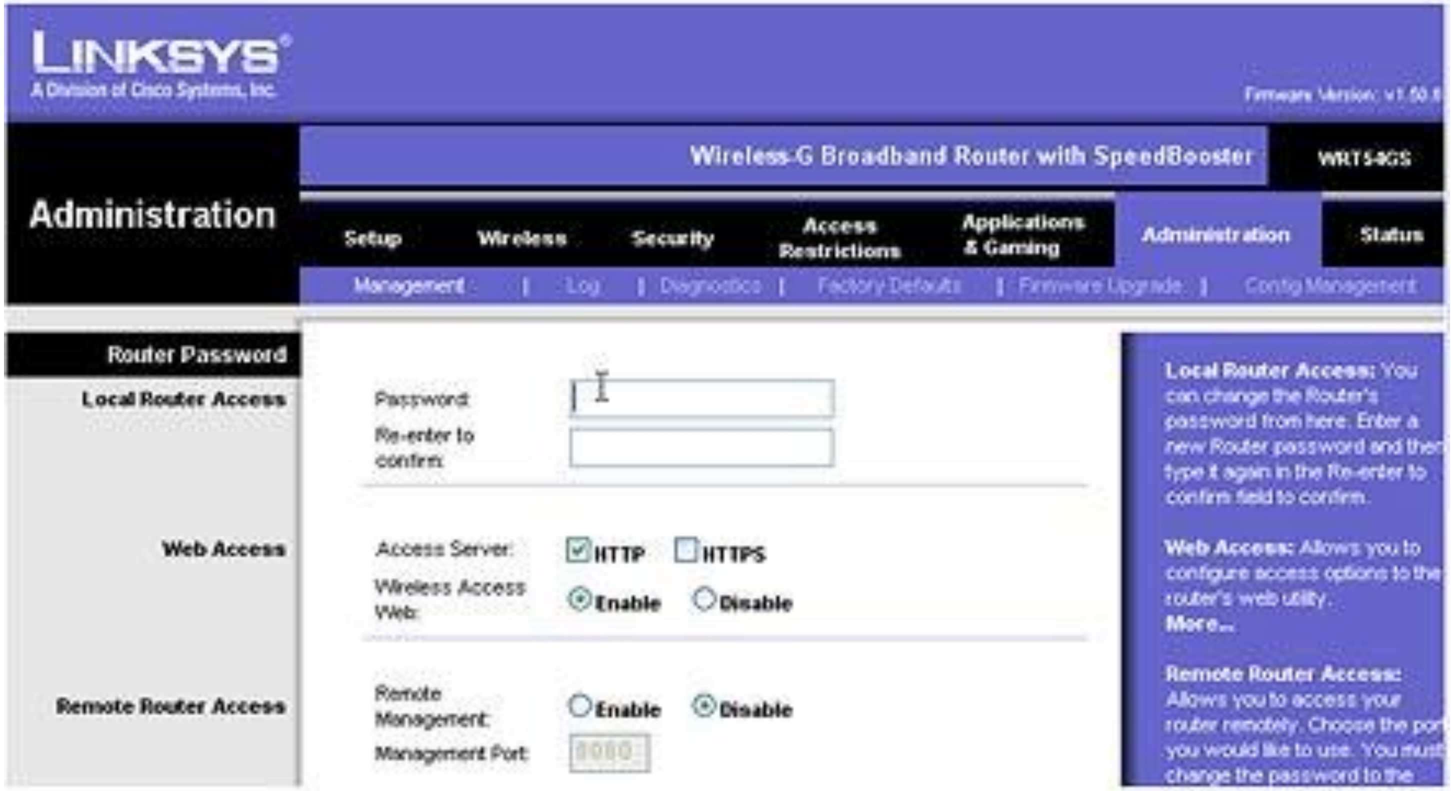
Password:

☐ Use Password Manager to remember this password.

OK Cancel

Accessing the router – Device manual will tell you default user name and password

Wireless Security Illustrated (2)


LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: v1.50.8
Wireless-G Broadband Router with SpeedBooster
WRT54GS
Administration
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management
Router Password

Local Router Access

Password:

Re-enter to confirm:

Web Access

Access Server: ☑ HTTP ☐ HTTPS

Wireless Access Web: ● Enable ○ Disable

Remote Router Access

Remote Management: ○ Enable ● Disable

Management Port: 8080

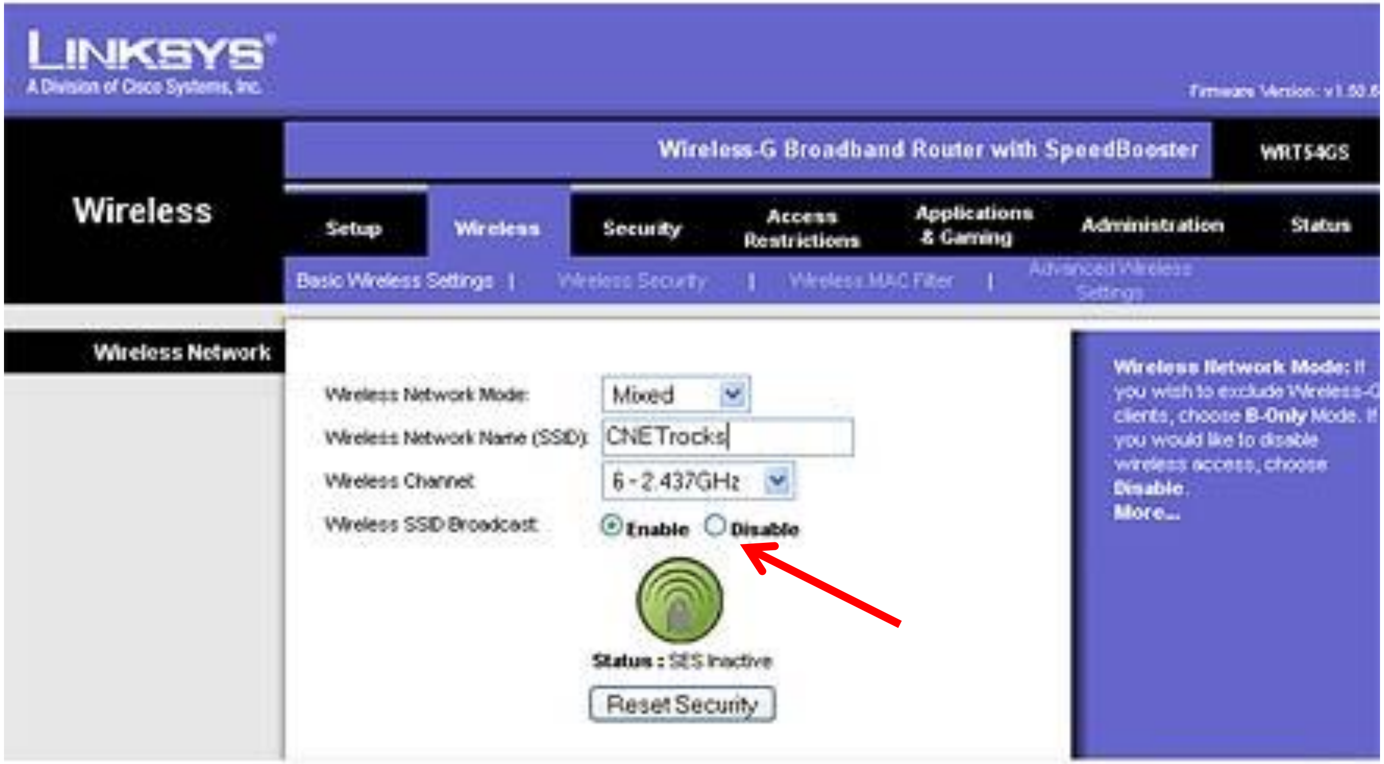
Local Router Access: You can change the Router's password from here. Enter a new Router password and the type it again in the Re-enter to confirm field to confirm.

Web Access: Allows you to configure access options to the router's web utility.
More...

Remote Router Access: Allows you to access your router remotely. Choose the por you would like to use. You must change the password to the

Immediately change the default administrator name and password!

Wireless Security Illustrated (3)



Wireless Network Mode: Mixed

Wireless Network Name (SSID): CNETrocks

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ● Enable ○ Disable

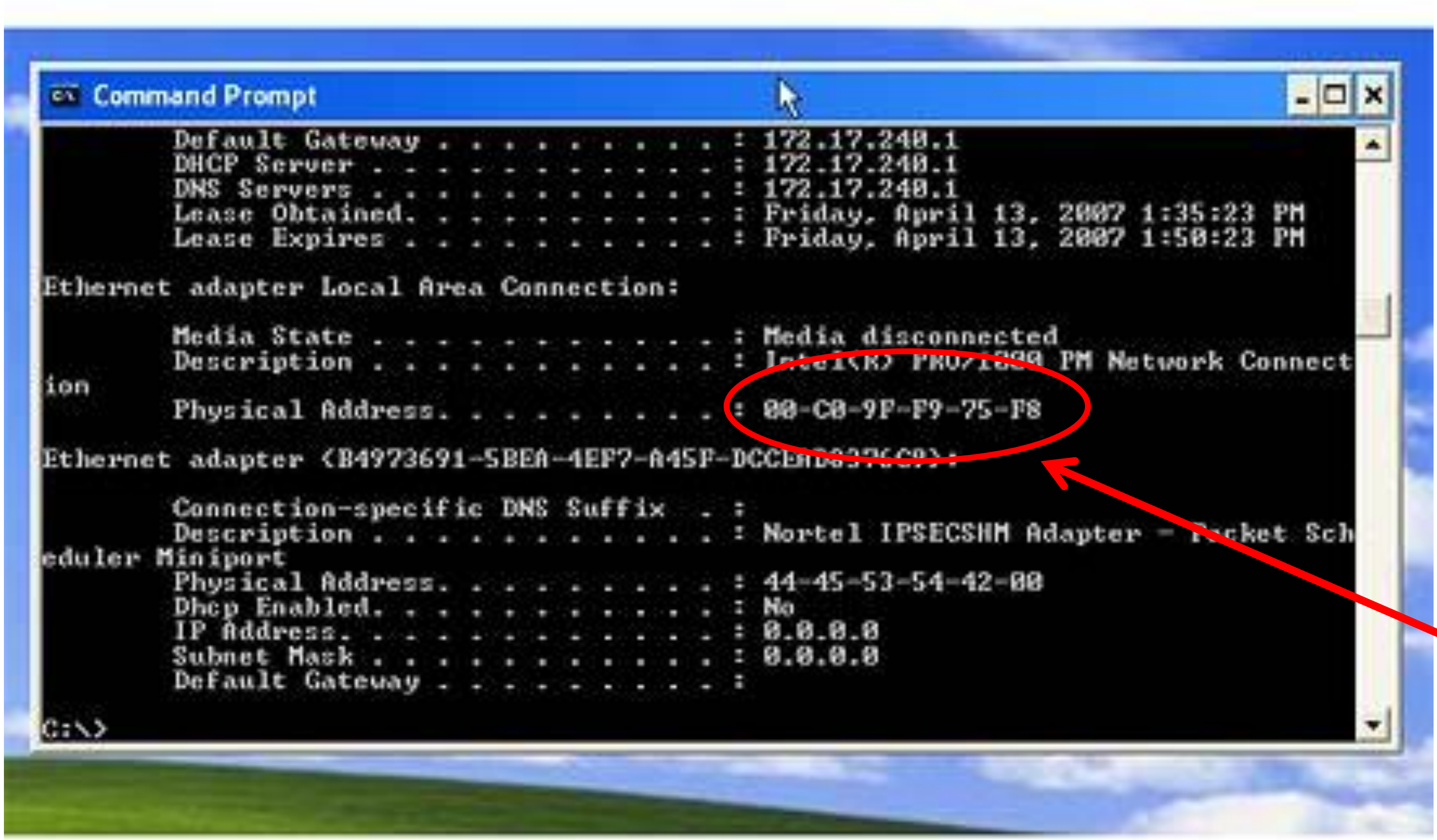
Status : SES Inactive

Reset Security

Wireless Network Mode: If you wish to exclude Wireless-G clients, choose **B-Only** Mode. If you would like to disable wireless access, choose **Disable**.
More...

Change the Default SSID and then disable broadcast

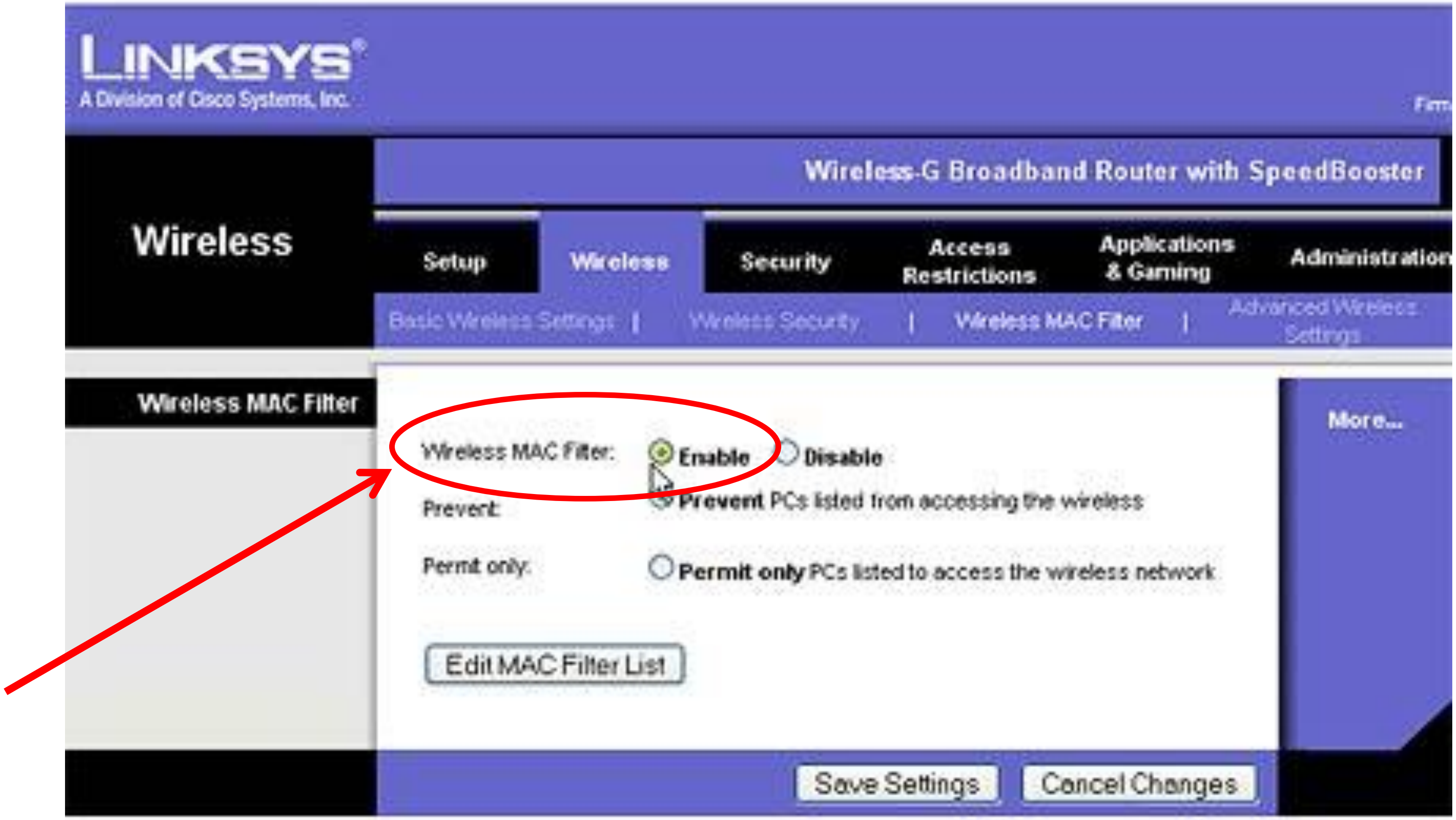
Wireless Security Illustrated (4)



```
        Default Gateway . . . . . . . . . : 172.17.240.1
        DHCP Server . . . . . . . . . . . : 172.17.240.1
        DNS Servers . . . . . . . . . . . : 172.17.240.1
        Lease Obtained. . . . . . . . . . : Friday, April 13, 2007 1:35:23 PM
        Lease Expires . . . . . . . . . . : Friday, April 13, 2007 1:50:23 PM

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Intel(R) PRO/1000 PM Network Connect
ion
        Physical Address. . . . . . . . . : 00-C0-9F-F9-75-F8

Ethernet adapter {B4973691-5BEA-4EF7-A45F-DCCEAD837CC8}:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Nortel IPSECSHM Adapter - Packet Sch
eduler Miniport
        Physical Address. . . . . . . . . : 44-45-53-54-42-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

Find the MAC addresses of all the devices on your network

Wireless Security Illustrated (5)



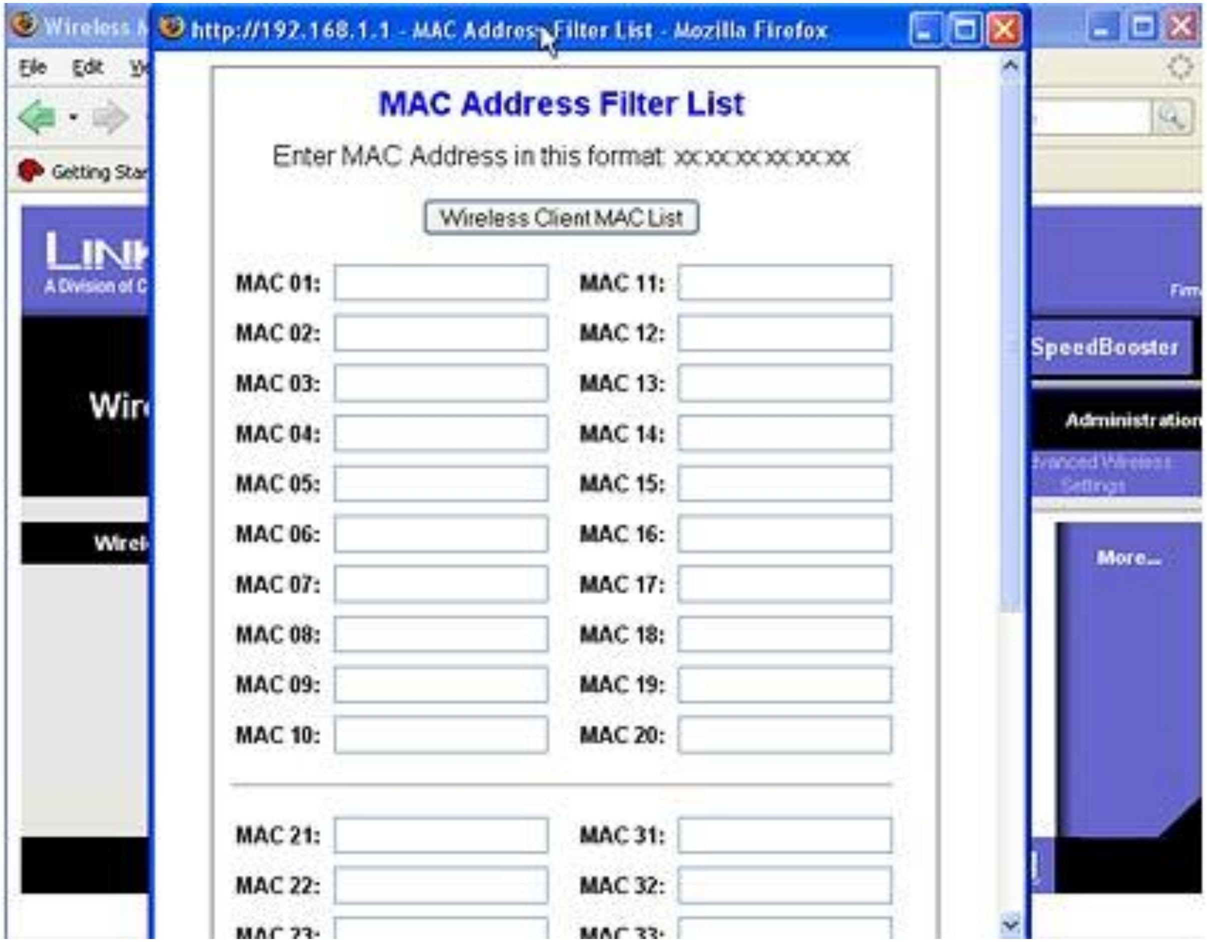
Wireless MAC Filter: ● Enable ○ Disable

Prevent: ○ **Prevent** PCs listed from accessing the wireless

Permit only: ○ **Permit only** PCs listed to access the wireless network

Enable MAC address filtering

Wireless Security Illustrated (6)



http://192.168.1.1 - MAC Address Filter List - Mozilla Firefox

MAC Address Filter List

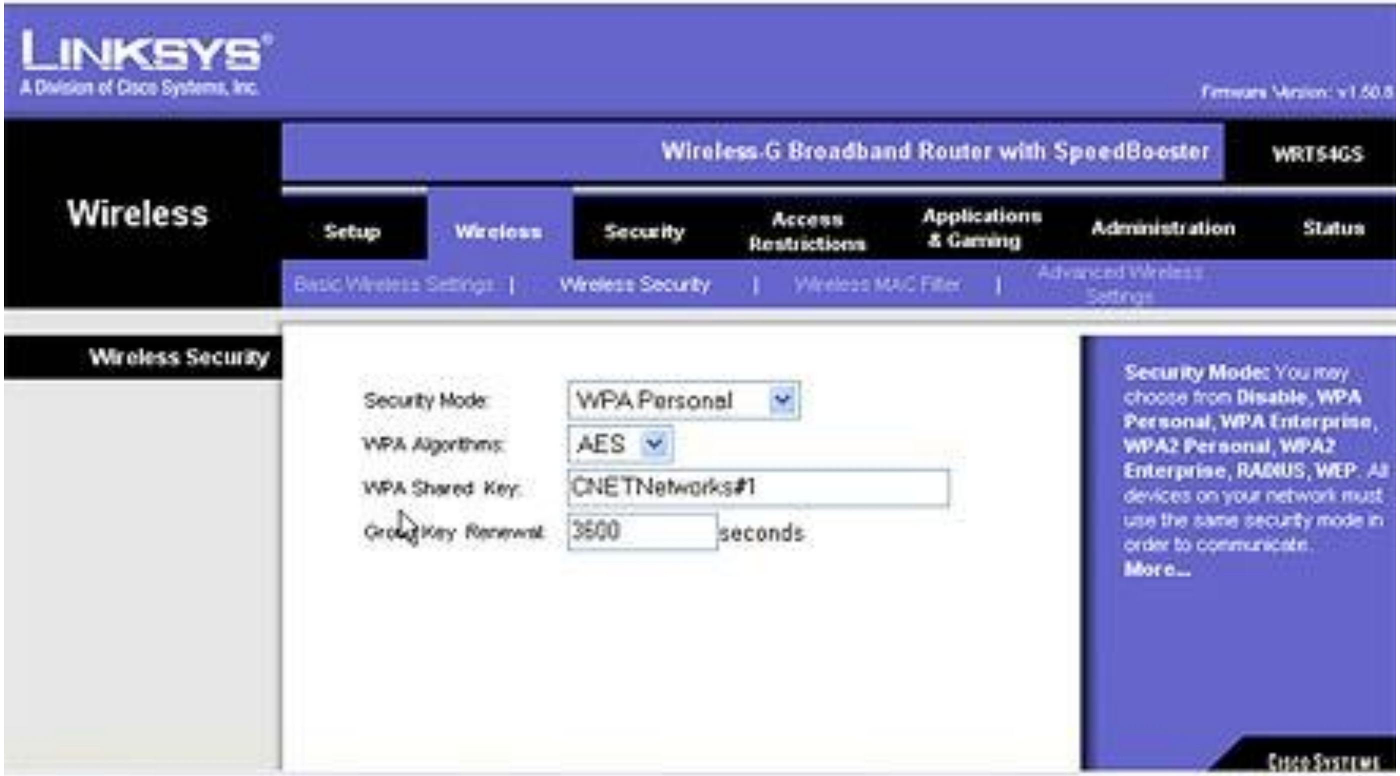
Enter MAC Address in this format: xxxxxxxxxxxx

Wireless Client MAC List

MAC 01:		MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	
MAC 21:		MAC 31:	
MAC 22:		MAC 32:	
MAC 23:		MAC 33:	

Add all of the MAC addresses from your networked devices

Wireless Security Illustrated (7)



Security Mode: WPA Personal

WPA Algorithms: AES

WPA Shared Key: CNETNetworks#1

Group Key Renewal: 3600 seconds

Security Mode: You may choose from **Disable, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, WEP**. All devices on your network must use the same security mode in order to communicate. **More...**

Set up WPA Encryption (Don’t forget to write this down!)

Securing Wireless Routers

(A couple more thoughts)

- WEP is better than nothing
  - If your device doesn’t support WPA at least use WEP encryption
  - Use a strong encryption key (no consecutive numbers or easy words)
  - Change your encryption key often
- Reduce your WLAN transmitter power
  - Not available in all models
  - If available you can reduce the range so it isn’t accessible outside your home or office
- Disable remote administration
  - Router may allow you to administer it via remote access
  - Only use this if it lets you define specific IP address(es) that can access the router

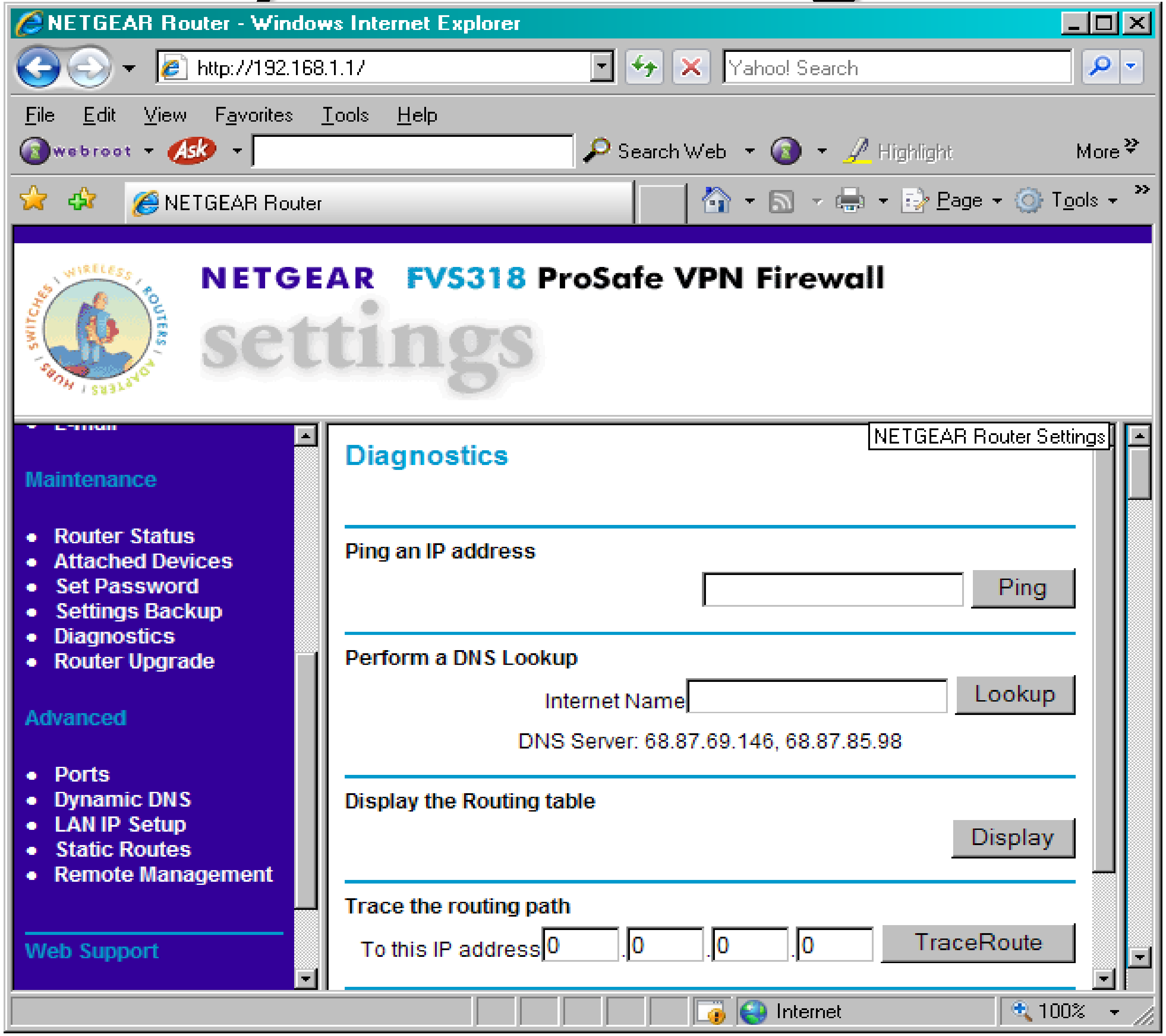
Best Practices

- Upgrades and Patches
  - Setup your routers and firewalls for automatic updates if available
  - Otherwise, set a schedule to check for updates
  - Update firmware as well as configuration or operating applications
- Backups
  - Backup your configuration information
  - Backup firewall logs to CD or USB – store offline
- Documentation
  - Network diagram!
  - All configuration information
  - User names, passwords and encryption keys
    - Keep in safe place (not on sticky notes or under your mouse pad!)
  - Mac addresses of all connected devices

Troubleshooting

- Check router/firewall WAN settings; refresh them with a new DHCP lease from your ISP
  - Sometimes DHCP loses its mind
- Ping – send "are you there?" packets
  - Useful for checking whether you have connectivity
- Tracert – follow a packet's path from source to destination
  - Tells you where connectivity stops
- Nslookup – look up information from DNS servers
  - Lots of useful information
- Ipconfig /all | more – see the IP configuration of a Windows system (and paginate the output)
  - See and understand the configuration of your system

Router/Firewall Diagnostics



NETGEAR Router - Windows Internet Explorer

http://192.168.1.1/

NETGEAR FVS318 ProSafe VPN Firewall

settings

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup
- Diagnostics
- Router Upgrade

Advanced

- Ports
- Dynamic DNS
- LAN IP Setup
- Static Routes
- Remote Management

Web Support

Diagnostics

NETGEAR Router Settings

Ping an IP address

[ ] Ping

Perform a DNS Lookup

Internet Name [ ] Lookup

DNS Server: 68.87.69.146, 68.87.85.98

Display the Routing table

Display

Trace the routing path

To this IP address 0 .0 .0 .0 TraceRoute

Final list ‘o tips

- Use a hardware firewall
  - It might be your wireless AP
- Manage DHCP and DNS
  - Restrict size of address pool
  - Use MAC address filtering
- Use WPA or WPA2 encryption; WEP if nothing else
- Document administrative credentials, pass phrases
- Make a network diagram
- Keep firmware updated and your configuration backed up
- Log activities and monitor logs

Q/A

Thank You!

City of Seattle

Office of Information Security

ois@seattle.gov